成都信息工程大学考试试卷

2020 —— 2021 学年第 二 学期

课程名称：病毒原理与防范　　使用班级：信安19级

试卷形式：开卷[ ]闭卷[√]

试题	一	二	三	四	五	总分
得分						

一、单项选择题答案	第1题	第2题	第3题	第4题	第5题	第6题	第7题	第8题
	第9题	第10题	第11题	第12题	第13题	第14题	第15题	

二、判断题答案	第1题	第2题	第3题	第4题	第5题	第6题	第7题	第8题	第9题	第10题

一、单项选择题（每小题2分，共30分，答案写在试卷开头相应位置处）

1. Worm.Sasser.f 属于哪种类型的病毒？（ ）

A. 系统病毒　　B. PE文件型病毒

C. 蠕虫病毒　　D. 引导型病毒

2. 节表中，表示节的名称的数组长度是？（ ）

A. 5字节　　B. 4字节

C. 12字节　　D. 8字节

3. 在DOS MZ头中偏移几字节处的值指示了PE文件头部？（ ）

A. 3CH字节　　B. 4CH字节

C. 5CH字节　　D. 6CH字节

4. 已知某节的实际大小为290H字节，该PE文件的FileAlignment为300H字节，SectionAlignment为1000H字节，则该节在内存中对齐后的大小为：（ ）

A. 290H字节　　B. 300H字节

C. 590H 字节　　D. 1000H 字节

5. PE 文件一般每个节都有自己属性，由属性代码来表示，若一个节的属性为可读可写，包含代码，则其属性为：（　　）

A. C0000020h　　B. 40000020h
C. 80000020h　　D. A0000020h

6. IAT 表在 PE 文件加载内存前后内容会发生变化，IAT 表项在文件中和在内存中存放的信息分别是：（　　）

A. 函数地址，函数名称　　B. 函数名称，函数地址
C. DLL 列表，函数名称　　D. 函数名称，DLL 列表

7. 在一个 PE 文件中，NumberOfSection 对应的两个字节的数据用 Byte 类型表示是：\x10\x00，说明该 PE 文件（　　）

A. 有 16 个节表　　B. 有 10 个节表
C. 有 16 个引入表　　D. 有 10 个引出表

8. 数据目录 DataDirectory 中每个表项(结构体)占的字节是？（　　）

A. 5 字节　　B. 6 字节
C. 7 字节　　D. 8 字节

9. 下列哪一项内容属于引导型病毒常用的技术手段？（　　）

A. 常驻内存高端　　B. 感染硬盘
C. 修改 BIOS　　D. 替换 DPT 表

10. 动态获取 API 函数地址时需要用到的两个函数 LoadLibrary 和 GetProcAddress，这两个函数位于哪个模块中？（　　）

A. user32.dll　　B. kernel32.dll
C. cmcfg32.dll　　D. netapi32.dll

11. 主引导扇区中的 DPT 表部分占多少字节？（　　）

A. 445 字节　　B. 446 字节
C. 64 字节　　D. 66 字节

12. 下列哪一项不是木马自启动常用的技术？（　　）

A. DLL 劫持　　B. 写注册表
C. 注册系统服务　　D. 把木马 EXE 放在 system32 目录下

13. 木马的主要特点是隐藏，以下不属于木马隐藏技术的是？（　　）

A. 通信隐藏　　B. 进程隐藏
C. 物理隐藏　　D. 服务隐藏

（　　）

14. 下列不属于木马软件结构的是？
A. 配置程序　　B. 木马服务器
C. 木马客户端　　D. 建立连接

（　　）

15. 查看本机端口及建立连接信息的命令是？
A. ipconfig　　B. net user
C. netstat　　D. cmd

二、判断题（对的打√，错的打×，每题2分，共20分，答案写在试卷开头相应位置处）

1. Windwos 平台下的动态链接库（.dll）文件不属于 PE 文件。（　　）
2. PE 文件的内存对齐粒度和文件对齐粒度总是相等的。（　　）
3. 可以通过节的名称获取节的属性信息，即可以通过节的名称获得节是否可读、可写和可执行等信息。（　　）
4. 某分区表项的第2个字节是80H，说明该表项对应的分区是活动分区。（　　）
5. 采用 CHS 寻址方式的硬盘，磁头数目的最大值是255。（　　）
6. 8086 CPU 实模式下，最大可寻址 1MB 的内存空间。（　　）
7. 主引导扇区位于硬盘的0柱0面1扇区。（　　）
8. 系统在启动过程中，主引导记录会被 BIOS 加载到 0x7C00 的位置执行。（　　）
9. Shellcode 一般是作为数据形式发送给服务器，制造溢出得以执行代码并获取控制权的，它不具备重定位的能力。（　　）
10. 木马可以基于 HTTP 协议建立秘密通信的信道。（　　）

三、填空题（每空1分，共10分）

1. 硬盘 CHS 寻址方式中，C 表示：_____，H 表示：_____，S 表示：_____。

2. 木马入侵的基本过程是配置木马、_____、_____、_____、建立连接、和远程控制。

3. 系统启动时首先 BIOS 加电自检，此时电源稳定后，CPU 从内存地址 FFFF:_____处开始执行，接下来会将硬盘第一扇区 MBR 读入内存地址 0000:7C00 处，之后检查地址(WORD)0000：_____是否等于 0xaa55，若不等于则转去尝试其他启动介质。

4. 在 DOS 实模式下，记录基本内存大小的容量标志单元的偏移是：0000：_____H。

学院_____　班级_____　姓名_____　学号_____　密封线内不答题

5. fs寄存器指向当前线程的TEB，则fs:[30]指向的当前进程的_____

四、简答题（每小题分值见各小题，共20分）

1. 手工往一个PE文件中插入一个新节，需要在PE文件中进行哪些操作，请简略描述主要步骤及需要更改的关键信息。（本题6分）

答：

2. 简述缓冲区溢出的基本原理，并绘制出溢出发生时栈内的变化情况。（本题6分）

3. PE 文件型病毒主要的技术手段有两个，它们分别是重定位和动态获取 API 函数地址。请简述为什么需要重定位和动态获取 API 函数地址？（4 分）写出重定位的相关汇编代码，并加以解释（4 分）（本题 8 分）

学院 班级 姓名 学号 密封线内不答题

五、综合分析题（每小题分值见各小题，共 20 分）

1.现有一 PE 文件，用文件查看工具打开的数据如下图所示，请按照要求填空。（本题 5 分，每空 1 分）

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	4D	5A	C1	D6	B4	BA	C7	BE	00	00	00	08	97	25	37	09
00000010	00	00	30	30	FB	3A	70	69	67	6A	20	20	2C	D1	A7	BA
00000020	C5	3A	67	75	6F	6A	70	65	6E	67	30	30	30	38	29	00
00000030	50	45	00	00	4C	01	00	00	55	55	55	55	30	00	00	00
00000040	55	55	55	55	70	00	0F	01	0B	01	6B	65	72	6E	65	6C
00000050	33	32	2E	64	6C	6C	00	55	88	00	00	00	00	00	00	00
00000060	00	00	00	00	00	00	40	00	04	00	00	00	04	00	00	00
00000070	68	C8	00	40	00	EB	03	55	04	00	68	02	00	40	00	EB
00000080	0D	02	00	00	B8	00	00	00	6A	40	EB	E4	02	00	6A	00
00000090	FF	15	EC	00	40	00	6A	00	FF	15	B4	00	40	00	55	55
000000A0	00	00	00	00	0D	00	00	00	55	55	55	55	55	55	55	55
000000B0	FC	00	00	00	DE	00	00	00	00	00	00	00	4D	65	73	73
000000C0	61	67	65	42	6F	78	41	00	4D	79	6D	69	6E	69	45	58
000000D0	45	2C	73	69	7A	65	3A	32	38	39	42	00	00	00	00	00
000000E0	45	78	69	74	50	72	6F	63	65	73	73	00	BA	00	00	00
000000F0	00	00	00	00	BA	00	00	00	EC	00	00	00	55	55	55	55
00000100	00	00	00	00	55	55	55	55	4A	00	00	00	B4	00	00	00
00000110	75	73	65	72	33	32	2E	64	6C	6C	00	00	10	01	00	00
00000120	EC	00	00	00	47	65	74	50	72	6F	63	41	64	64	72	65
00000130	73	73	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

（1）PE 头部的 RVA 是：_____；

（2）该 PE 文件中节的数目是：_____；

（3）数据目录在文件中的偏移是 0xA8，则第一张导入表的 RVA 是：_____；第二张导入表的 RVA 是：_____。

（4）该 PE 文件的内存对齐粒度是 04H，文件对齐粒度是 04H。该 PE 文件是否存在 FOA 到 RVA 的转换问题？：_____。（答“是”、“否”）

2. 某引导型病毒将原来硬盘的主引导扇区备份至了硬盘的第 10 个扇区，同时将硬盘上的第 1 个扇区的内容替换成了病毒的代码。请你调用中断程序，编写一段清除该病毒的程序代码，假设当前段寄存器 cs=ds=es=0。（int 13h 中断，相关参数的解释参考如下：AH＝02H 表示读扇区，AH＝03H 表示写扇区；AL 表示扇区数；CH 表示柱面；CL 表示扇区；DH 表示磁头；DL 表示驱动器，值为 00H~7FH 为软盘；值为 80H~0FFH 为硬盘；ES:BX 表示缓冲区的地址。）（本题 5 分，每空 0.5 分）

```
代码 1：  MOV ax, _____;（1）
          MOV bx, _____;（2）
          MOV cx, _____;（3）
          MOV dx, _____;（4）
          Int _____;（5）
```

```
代码 2：  MOV ax, _____;（6）
          MOV bx, _____;（7）
          MOV cx, _____;（8）
          MOV dx, _____;（9）
          Int _____;（10）
```

3. 下面是动态获取 API 函数的部分代码，请在横线上填空完善代码，相关数据结构的定义参考题后附图（每空 1 分，共 10 分）

```
.code
main:
Start:
        mov   esi, _____;(1)
        and   esi,0ffff000h
LoopFindKernel32:
        sub   esi,1000h
        cmp   word ptr[esi], _____;(2)
        jnz   short LoopFindKernel32
GetPeHeader:
        mov edi,dword ptr[esi+_____];(3)
        add edi, esi
        cmp word ptr[edi],_____;(4)
      jnz short LoopFindKernel32
      mov Kernel32Addr,esi
      invoke GetApiAddress,Kernel32Addr,addr aLoadLibrary
      mov LoadLibraryAddr,eax
      invoke GetApiAddress , Kernel32Addr, addr aGetProcAddr
      mov GetProcAddr , eax
      invoke MessageBoxA,0,addr temp2,addr szTitle,0
      invoke ExitProcess,0
    mov esi,hModule
    add esi,[esi+3ch]
```

```
assume esi:ptr IMAGE_NT_HEADERS
mov esi,[esi]._____;(5)
add esi, _____;(6)
assume esi:ptr IMAGE_EXPORT_DIRECTORY
mov ebx,[esi]._____;(7)
add ebx,hModule
xor edx,edx
.repeat
    push esi
    mov edi,[ebx]
    add edi,hModule
    mov esi,szApiName
    mov ecx,dwApiLength
    cld
    repz cmpsb
    .if ZERO?
        pop esi
        jmp _Find_Index
    .endif
    pop esi
    add ebx,4
    inc edx
    .until edx >= [esi]._____;(8)
    jmp _Exit
    _Find_Index:
        sub ebx,[esi].AddressOfNames
        sub ebx,hModule
        shr ebx,1
        add ebx, [esi]._____;(9)

        add ebx,hModule
        movzx eax,word ptr [ebx]
        shl eax,2
        add eax,[esi]._____;(10)
        add eax,hModule
        mov eax,[eax]
        add eax,hModule
        mov dwReturn,eax
    _Exit:
```

学院_____班级_____姓名_____学号_____ ……密封线内不答题……